Landesamt für Sicherheit in der Informationstechnik

LSI-Info T#07

BOS-ALARMIERUNGSSYSTEME

Version 1.0 vom: 13.08.2021

Management Summary

Mit der Digitalisierung des Behördenfunks wurden neue Alarmierungswege eröffnet. Die Alarmierungen des nicht-polizeilichen BOS-Bereichs[1)] (nPol-BOS) - also Feuerwehren (Fw), Katastrophenschutz (KatS), Rettungsdienst (RD) mit den freiwilligen Hilfsorganisationen (ASB, BRK, DLRG, JUH, MHD) und Technisches Hilfswerk (THW) - erfolgen durch die Integrierten Leitstellen zum Großteil analog. Die digitale Alarmierung befindet sich noch in der Erprobungsphase.

Das Gefährdungspotenzial der Systeme zur Verarbeitung dieser Funksignale - vor allem der alten analogen Signale - ist weithin bekannt, wird aber durch die Betreiber vor Ort nicht immer wahrgenommen oder unterschätzt. Das macht solche Alarmierungssysteme für unbefugte Einsichtnahme oder Angreifer interessant. Hauptproblem sind hier vor allem Einstellungen, die zu einer unsicheren Systemumgebung führen.

Nachstehend folgen mit der Staatlichen Feuerwehrschule Geretsried abgestimmte Empfehlungen, wie nPol-BOS-Alarmierungssysteme besser abgesichert werden können.

1) BOS = Behörden und Organisationen mit Sicherheitsaufgaben

Vorbemerkung:

Zur Funk-Alarmierung bei Fw, KatS, RD und THW kommen Systeme zur Verarbeitung von Funk-Codes - z. B. analoge ZVEI- und digitale FMS- oder POCSAG-Telegramme [2] - zum Einsatz.

2) POCSAG = *Post Office Code Standard Advisory Group*

Ein Computersystem bekommt von einem daran angeschlossenen Funkgerät (Analog/Digital) oder einem Alarmierungsfunkmelder BOS-Radiosignale aus dem BOS-Funknetz und entschlüsselt diese Daten mittels eines gültigen Radio Identification Codes (RIC).

Die entschlüsselten Daten können dann durch Systeme wie *BosMon, FE2, FF-Agent* oder *FMS32* eingesehen werden. Technisch ist auch das Mithören des Sprachfunks und die Weiterleitung von Alarmierungen an Apps auf Mobiltelefonen möglich. Beispielsweise kann das System *TETRAcontrol* zur Datenweitergabe an BosMon-Webserver genutzt werden.

Unsichere Konfigurationen vermeiden, Systeme stehen im Fokus

Die Vergangenheit hat gezeigt, dass sich einige Betreiber nur unzureichend um die Sicherheit ihrer Server gekümmert haben. Solche Server sind über Suchdienste wie z. B. censys oder shodan leicht auffindbar. Damit waren Einsichtnahmen in Einsatzdaten und sehr persönliche Daten durch eine interessierte Öffentlichkeit und potenzielle Angreifer ohne weiteres möglich.

Die Computerzeitschrift c't hat 2020 einen Artikel mit dem Titelthema „BOS-Scheunentor - Unverschlüsselte Rettungsdienst-Nachrichten im Internet“ veröffentlicht.[3]
Seitdem stehen nPol-BOS-Systeme noch stärker im Fokus.

3) c't Magazin für Computertechnik, Heft 23/2020, Seite 26 f
Titel c't deckt auf: BOS-Server, BOS-Scheunentor Unverschlüsselte Rettungsdienst-Nachrichten im Internet
https://www.heise.de/select/ct/2020/23/2024809442273661482

Empfehlungen:

Aufgrund der Schutzwürdigkeit der darüber weitergemeldeten Daten sollten BOS-Systeme von entsprechend qualifiziertem Personal besonders sorgfältig konfiguriert werden.

Bitte berücksichtigen Sie die Empfehlungen der Softwarehersteller.
Für BosMon-Systeme beachten Sie bitte
https://www.bosmon.de/doc/bosmon/1.5/howto/webserver.html
https://www.bosmon.de/doc/bosmon/1.5/cfg/webserver.html

Ein Zugriff sollte nur über HTTPS basierend auf einem SSL-Zertifikat sowie nur mit einer entsprechenden Authentifizierung zulässig sein.
Keinesfalls sollte das System offen im Internet erreichbar sein, da u. a. die obengenannten Suchdienste diese Systeme auffinden.

In der Benutzerverwaltung der BOS-Systeme sollten starke Passwörter verwendet werden. Die Nutzer sollten nur ihren Aufgabenbereich sehen können. Von der Verwendung eines Gast-Benutzers wird eindringlich abgeraten.

Ebenfalls ist es ratsam, die Alarmauswertung zur Weiterleitung auf andere Geräte so zu konfigurieren, dass keinerlei personenbezogene Daten einsehbar sind.

Zur Erhöhung der Sicherheit sollte die Option zur Aktivierung einer Protokolldatei genutzt werden. Die Protokolldatei sollte regelmäßig auf Auffälligkeiten überprüft werden und möglichst auch auf einem anderen System verfügbar sein.

Der Server und das BOS-System sollten aktuell gehalten werden:
Informieren Sie sich über Patches und Sicherheitslücken, z. B. über ein Newsletter-Abonnement des Herstellers. Sobald ein Hersteller für eine Schwachstelle einen Patch bzw. Update zur Verfügung stellt, sollten diese zeitnah installiert werden, um die Sicherheitslücke zu schließen. Veröffentlichte Sicherheitslücken sind schnell öffentlich bekannt und es dauert oft nicht lange bis Schadsoftware vorliegt, die diese Sicherheitslücke ausnutzt.
Für Betriebssysteme werden Sicherheitsupdates nur eine gewisse Zeit zur Verfügung gestellt. Berücksichtigen Sie diesen Supportzeitraum bereits bei der Planung und ersetzen Sie Systeme, für die es keinen Support mehr gibt.
Weiterführende Informationen zum Patchmanagement entnehmen Sie bitte dem LSI-Info T#08.

Sorgen Sie für eine entsprechende Datensicherung, auch der Konfigurationsdateien, z. B. der bosmon.cfg.

Betreiben Sie den BOS-Rechner in einer physisch gesicherten Umgebung (Serverraum), zu der nur autorisiertes Personal Zutritt hat und welche gegen äußere Einflüsse geschützt ist. Eine unterbrechungsfreie Stromversorgung ist ratsam.

Aktivieren Sie die benötigten Schnittstellen und Funktionen nach dem Minimalprinzip. Sicherheitsrelevante Systemeinstellungen des BOS-Rechners, wie die Startreihenfolge der Laufwerke im BIOS/UEFI sollten mit einem Kennwort vor Manipulationen geschützt werden.

Prüfen Sie bei der Aufstellung von Monitoren und Info-Terminals in öffentlich einsehbaren Bereichen (z. B. Fahrzeughalle), dass keine personenbezogenen Daten von nicht autorisierten Personen / Passanten eingesehen werden können.

Bei der Entsorgung von BOS-Systemen sollten Sie eine sichere Datenlöschung gewährleisten. Dies kann notfalls auch durch die Zerstörung der HDD oder SSD in kleinste Teile erfolgen.

Bitte sichern Sie Test- oder Schulungssysteme ebenfalls entsprechend ab, um Angreifern keine Zugangs- oder Informationsmöglichkeiten zu geben.

KONTAKT

Weitere Informationen finden Sie unter:

https://lsi.bayern.de/kommunen/

Für Unterlagen und Beratung wenden Sie sich bitte per E-Mail an:

Beratung-Kommunen@lsi.bayern.de.

Gerne ist das kommunale Beratungsteam auch telefonisch unter 0911/215 49 - 523 für Sie erreichbar.